IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Solomon W. Golomb, et al. Art Unit : 2164
Serial No.: 09/576,598 Examiner : Belix Ortiz
Filed : May 22, 2000
Title : ENCRYPTION SYSTEM BASED ON CROSSED INVERSE QUASIGROUPS

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Sir:

Applicants herewith file this appeal brief under Rule 37, thereby perfecting the notice of appeal that was originally filed on September 6, 2006.

Important note: this case was discussed with the Examiner, and during the discussion, the case was indicated as allowed. Appendix 1 shows the PAIR sheet indicating the case as allowed, but Notice of Allowance not yet mailed. Subsequently, the PAIR database was changed and no longer indicates the case as allowed. There also shows an interview summary record of the interview that was carried out on September 13, 2006. An interview summary has never appeared in the image file wrapper.

Since the appeal date has never been satisfied, the undersigned feels that there is no alternative but to perfect the notice of appeal, since the current claims are quite clearly allowable.

The sections required by Rule 41.37 follow.

(1) Real Party in Interest

University of Southern California is the 100% assignee of this application and is hence the real party in interest.

(2) Related Appeals and Interferences

There are no known related appeals or interferences.

(3) Status of Claims

Claims 1, 3-16, 19, 21-26, 29, 31-33, 35 and 36 are rejected and each of these claims are herewith appealed. Claims 2, 17-82, 20, 27-28, 30 and 34 have been canceled.

(4) Status of Amendments

An amendment after final was filed on September 6, 2006. It is presumed that this amendment was entered.

(5) Summary of Claimed Subject Matter

The present application teaches a cryptography method which determines information that is to be encrypted. It encrypts the information using a key. See page 9 of the specification lines 22-25. See also page 8 lines 24-25. A nontrivial ci-quasigroup is used as the key. See page 7 line 11 through page 8 line 10.

A quasigroup has properties that any two elements have an operation "*" which is also within the quasigroup, and also that there is a permutation that decodes the encryption. See page 8 lines 4-10.

Claim 19 defines a cryptography method that determines information to be encrypted, and encrypts that using the key. See page 8 lines 24-25, and page 9 lines 22-25. Claim 19 also describes characteristics of the quasigroup, described at page 7 line 11 through page 8.

Claim 29 defines an apparatus that encrypts a message into an encrypted message using the key. See page 8 lines 24-25 and page 9 lines 22-25. The key has characteristics of values from operations within the group also being within the group, and has a permutation. See page 7 line 11 through page 8 line 10.

(6) Grounds of Rejection to be Reviewed on Appeal

Are Claims 1, 3-16, 19, 21-22, 29, 31-33 and 35-36 properly rejected under 35 USC 112, second paragraph as being indefinite?

Are Claims 1, 3-16, 19, 21-26, 29, 31-33 and 35-36 properly rejected under 35 USC 101 as being directed to non-statutory subject matter?

The changes made to many of the claims in the amendment after final (which is presumed to have been entered) obviates

the rejections under 35 USC 112, second paragraph except for the rejection to Claim 21.

(7) Argument

The objection to Claim 21 is respectfully traversed, since Claim 19 refers to the "crossed inverse quasigroup" as "the quasigroup". Hence, the reference to "said quasigroup" in Claim 21 is completely correct.

The claims stand rejected under 35 USC 101 as allegedly being directed to nonstatutory subject matter. These contentions are respectfully traversed for reasons set forth herein. In each of the claims, first of all, information is encrypted and hence changed by the encryption. As such, there is physical transformation of the information. There is also a useful concrete and tangible result since the claims recite changing something to a different state or thing: an encrypted message.

The rejection states that the claimed invention is "directed to an arbitrary math technique". However, this claim does not preempt or attempt to preempt any kind of algorithm. It defines forming encrypted information based on information to be encrypted. As such, it is not directed to solely a mathematical algorithm, and does not simply manipulate abstract

ideas. There is clearly a practical application, since it is forming encrypted information. As such, the rejection under 35 USC 101 is respectfully traversed and the Examiner's rejection should be reversed.

Please apply the appeal brief fee of $250, the 3 month extension of time fee of $510, and any other outstanding charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: February 2, 2007

Scott C. Harris
Reg. No. 32,030

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

10705398.doc

Appendix of Claims

1. A cryptography method, comprising:

determining information M to be encrypted; and

encrypting said information to form encrypted information using a non-trivial ci-quasigroup as a key K to create a cypher C indicative of the information M as C = M*K, where * denotes a mathematical operation, where the non-trivial ci-quasigroup has properties that for the operation *, between any two elements in the non-trivial ci-quasigroup, a result of the operation is also in the non-trivial ci-quasigroup and for every K, as M takes on a different value, [[the]] resulting values of C are each distinct, for every M, as K takes on all key values, the resulting values of C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

2. (Canceled).

3. A method as in claim 1, further comprising decoding said information using a crossed-inverse function of said non-trivial ci-quasigroup.

4. A method as in claim 1, wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result, and iterating said encryption an arbitrary number of times.

5. A method as in claim 1 further comprising defining a rule indicative of said non-trivial ci-quasigroup.

6. A method as in claim 3 further comprising defining a rule indicative of said crossed inverse function of said quasigroup.

7. A method as in claim 1 further comprising carrying out a second encrypting using said mathematical operation, and wherein a result of said second encryption is encrypted exponentially more than a result of a first encryption.

8. A method as in claim 1 wherein said encrypting comprises using a non trivial non-group crossed inverse quasigroup to encode.

9. A method as in claim 3 further comprising distributing information indicative of said non-trivial ci-quasigroup as a public key, and keeping secret the non-trivial ci-quasigroup.

10. A method as in claim 1 wherein said quasigroup is formed by an n by n square, where n is greater than 10^{10}.

11. A method as in claim 4 wherein said first and second encryption form iterative encipherment.

12. A method as in claim 4 wherein a first interation is carried out in a different direction than said first encryption.

13. A method as in claim 12 wherein a first direction of said first iteration is left to right and said different direction is right to left.

14. A method as in claim 1 wherein said encrypting is carried out using block ciphers.

15. A method as in claim 14 wherein said block cipher are defined by a function.

16. A method as in claim 14 wherein said block ciphers are formed using cross inversed quasigroups, used according to *C = f(M,K)* for the encryption and *M=finv(C,K)* for a decryption.

17-18. (Canceled).

19. A cryptography method, comprising:

determining information to be encrypted; and

encrypting said information M to form encrypted information using a Key K which is a crossed-inverse quasigroup to create a cipher C as C = M*K, where * denotes a mathematical operation, where the quasigroup has properties that for the operation *, between any two elements in the quasigroup, the result of the operation is also in the quasigroup, and for every K, as M takes on different values, the resulting values of the cipher C, are each distinct, for every M, as K takes on all key values, the resulting values of the cipher C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

20. (Canceled).

21. A method as in claim 19, further comprising decoding using a crossed inverse of said quasigroup.

22. A method as in claim 1, wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result.

23. A cryptography method comprising encrypting information using an arithmetic with an algebraic structure, said algebraic structure being a nongroup, nonfield structure.

24. A method as in claim 23 wherein said algebraic structure is not associative.

25. A method as claim 23 wherein said algebraic structure is not commutative.

26. A method as in claim 24 wherein said algebraic structure is not commutative.

27-28. (Canceled).

29. An apparatus comprising a program stored on a computer readable media including instructions to:

encrypt a message M into an encrypted message_using a key K indicative of a crossed-inverse quasigroup representation, where the quasigroup has properties that for an operation *, between any two elements in the quasigroup, a result of the operation is also in the quasigroup, and for every K, as M takes on message values, resulting values of a cipher C, where C = M*K are each distinct, for every M, as K takes on all key values, resulting values of the cipher C, are all distinct; and each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$;

send the encrypted message C; and

decrypt the encrypted message using information indicative of the same crossed-inverse quasigroup representation.

30. (Canceled).

31. An apparatus as in claim 29, wherein said operation is one which is based on a multiplication table which is expressed as a rule.

32. An apparatus as in claim 29, further comprising adding a random seed to said arithmetic.

33. An apparatus as in claim 29, further comprising using an additional encryption to provide an effective key size of x^2 of an original encryption.

34. (Canceled).

35. A method as in claim 1, further comprising sending the encrypted information as a message.

36. A method as in claim 19, further comprising sending the encrypted information as a message.

Evidence Appendix

None.

Related Proceedings Appendix

None.